

ICS 35.040



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 18336.1-2024

**Cybersecurity technology-Evaluation criteria for IT
security-Part 1: Introduction and general model**

网络安全技术 信息技术安全评估准则 第1部分：简介和一般模型

(English Translation)

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: SAMR; SAC

Table of Contents

Foreword	4
Introduction	6
1 Scope	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviated terms	35
5 Overview	36
5.1 General	36
5.2 The TOE	36
5.3 Target audience of ISO/IEC 15408	38
5.4 The different parts of ISO/IEC 15408	39
5.5 Evaluation context	40
6 General model	41
6.1 Introduction	41
6.2 Assets and countermeasures	41
6.3 Evaluation	46
7 Tailoring Security Requirements	47
7.1 Operations	47
7.2 Dependencies between components	50
7.3 Extended components	51
8 Protection Profiles and Packages	51
8.1 Introduction	51
8.2 Packages	51
8.3 Protection Profiles	52
8.4 Using PPs and packages	55
8.5 Using Multiple Protection Profiles	56
9 Evaluation results	56
9.1 Introduction	56
9.2 Results of a PP evaluation	57
9.3 Results of an ST/TOE evaluation	57
9.4 Conformance claim	57
9.5 Use of ST/TOE evaluation results	59

Annex A (Informative) Specification of Security Targets	60
Annex B (Informative) Specification of Protection Profiles	80
Annex C (Informative) Guidance for Operations	86
Annex D (Informative) PP conformance	90
Bibliography	92

Foreword

GB/T 18336 "Information technology - Security techniques - Evaluation criteria for IT security" includes the following 3 parts.

- Part 1: Introduction and general model;
- Part 2: Security functional components;
- Part 3: Security assurance components.

This Part is part 1 of GB/T 18336.

This Part is drafted in accordance with specifications in GB/T1.1-2009.

This Part shall replace GB/T 18336.1-2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

The main differences between this Part and GB/T 18336.1-2008 are as follows.

- "2 Normative references" is added;
- In "3 Terms and definitions", "3.2 Terms and definitions concerning development (ADV) class", "3.3 Terms and definitions concerning guidance documentation (AGD) class", "3.4 Terms and definitions concerning life cycle support(ALC) class", "Terms and definitions concerning vulnerability assessment (AVA) class" and "3.6 Terms and definitions concerning combination (ACO) class" are added;
- In "5 Introduction", "5.2 TOE" is added;
- The "IT product and system" to which GB/T 18336 is applicable is amended as "IT product";
- "5.1 Elements concerning security" and "5.2 Assurance method" are amended as "6.2 Asset and countermeasures" and "6.3 Evaluation" in this Part;
- "5.3 Security concepts" in GB/T 18336.1-2008 is removed;
- "5.4.1 Expression of security requirements" is re-edited as "7 Clipping security requirements" in this Part;
- "5.4.2 Evaluation types" in GB/T 18336.1-2008 is removed;

- "8 Protection profile and package" is added;
- "6 GB/T 18336 Requirements and evaluation results" is re-edited as "9 Evaluation results" in this Part;
- "Annex A Protection profile specification" is re-edited as "Annex B Protection profile specification" in this Part; "B.11 Protection profile of low level assurance" and "B.12 Referring to other standards in PP" are added;
- "Annex B Specification of security target" is re-edited as "Annex A Specification of security target" in this Part; "A.3 Using ST", "A.11 Problems solved by ST", "A.12 Security target of low level assurance" and "A.13 Referring to other standards in ST" are added.

This Part uses translation method to equivalently adopt the international standard ISO/IEC 15408-1:2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part1.Introduction and general mode".

The domestic documents that are consistently corresponding to the normative international references in this Part are as follows.

- GB/T 18336.2-2015 "Information technology - Security techniques - Evaluation criteria for IT security Part 2: Security functional components (ISO/IEC 15408-2:2008, IDT)"
- GB/T 18336.3-2015 "Information technology - Security techniques - Evaluation criteria for IT security Part 3: Security assurance components (ISO/IEC 15408-3:2008, IDT)"
- GB/T 30270 "Information technology - Security technology - Methodology for IT security evaluation (GB/T 30270-2013, ISO/IEC 18045:2005, IDT) this Part was proposed by and shall be under the jurisdiction of China Information Security Standardization Technical Committee (SAC/TC 260).

The main drafting organizations of this Part. China Information Technology Security Evaluation Centre, Information Technology Security Test and Evaluation Centre AND The Third Research Institute of Ministry of Public Security.

1 Scope

This Part of GB/T 18336 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408.It describes the various parts of the ISO/IEC 15408; defines the terms and abbreviations to be used in all parts of the ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. This Part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation method and the scope of evaluation schemes shall be provided in IT safety evaluation methodology.

2 Normative references

The articles contained in the following documents have become part of this document when they are quoted herein. For the dated documents so quoted, all the modifications (including all corrections) or revisions made thereafter shall be applicable to this document.

ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components
 ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components
 ISO/IEC 18045, Information technology - Security techniques - Methodology for IT Annex D (Informative) PP conformance
 D.1 Introduction A PP is intended to be used as a "template" for an ST. That is, the PP describes a set of user needs, while an ST that conforms to that PP describes a TOE that satisfies those needs.

Note that it is also possible for a PP to be used as a template for another PP. That is PPs can claim conformance to other PPs. This case is completely similar to that of an ST vs. a PP. For clarity this Annex describes only the ST/PP case, but it holds also for the PP/PP case.

ISO/IEC 15408 does not allow any form of partial conformance, so if a PP is claimed, the PP or ST must fully conform to the referenced PP or PPs. There are however two types of conformance ("strict" and "demonstrable") and the type of conformance allowed is determined by the PP. That is, the PP states (in the PP conformance statement, see B.5) what the allowed types of conformance for the ST are. This distinction between strict and demonstrable conformance is applicable to each PP to which an ST may claim conformance on an individual basis. This may mean that the ST conforms strictly to some PPs and demonstrably to other PPs. An ST is only allowed to conform to a PP in a demonstrable manner, if the PP explicitly allows this, whereas an ST can always conform with strict conformance to any PP.

Restating this in other words, an ST is only allowed to conform to a PP in a demonstrable manner, if the PP explicitly allows this.

Conformance to a PP means that the PP or ST (and if an ST is of an evaluated product, the product as well) meets all requirements of that PP.